SECNAV INSTRUCTION 5500.36A

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY SECURITY ENTERPRISE

Ref: See enclosure (1)

Encl: (1) References
       (2) Department of the Navy Security Enterprise Governance
       (3) Responsibilities
       (4) Definitions

1. Purpose

    a. Define the Department of the Navy (DON) Security Enterprise (SE) and assign responsibilities.

    b. Establish and issue policy to guide and manage the implementation of the DON SE pursuant to references (a) through (aj) located in enclosure (1).

    c. Provide a framework and guidance to promote efficiency and facilitate consistent security policies and practices across the DON.

    d. Establish the DON Security Enterprise Executive Committee (DON SE EXCOM) and provide direction for comprehensive DON SE policy, oversight framework, and governance structure that supports safeguarding personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. See enclosure (2) for information regarding the DON SE governance and enclosure (3) for information regarding the Senior Director for Security.

    e. Provide a common lexicon for the DON SE.

2. Cancellation. SECNAVINST 5500.36.

3. Responsibilities. See enclosure (3).

4. <u>Applicability</u>. This instruction:

a. Applies to all personnel employed by, detailed to, or assigned to the DON, including Government Civilians (both appropriated and non-appropriated funds); members of the active and reserve components of the U.S. Navy and U.S. Marine Corps; temporarily assigned forces performing a full-time or training role or function of security, e.g., Auxiliary Security Force and Ship's Self Defense Force; experts or consultants performing services for the DON through personnel appointments or contractual arrangements; industrial or commercial contractor, licensee, certificate holder, or grantee, including subcontractors.

b. Will not alter or supersede the existing authority and policies of the Director of National Intelligence (DNI) regarding the protection of intelligence sources, methods, and activities pursuant to reference (p), or the authorities delegated by the DNI to the Heads of the Intelligence Community Element.

c. Does not apply to Nuclear Weapons Security Programs which are administered pursuant to references (o) and (ah).

d. Does not alter or supersede oversight, management, and authority over resources for Special Access Programs (SAP) found in references (x) and (z).

e. Does not supersede or change responsibilities and authorities of the Director, Naval Nuclear Propulsion Program (N00N), established by 50 U.S.C. §2406 and §2511 (codifying Executive Order 12344, 1 February 1982).

f. Does not apply to the authorities of the DON SE EXCOM regarding law enforcement policy and antiterrorism and/or force protection, and will not alter or supersede existing service or organizational missions specifically assigned to those entities, e.g. Naval Criminal Investigative Service (NCIS), Headquarters Marine Corps.

g. Does not alter or supersede oversight, management, and authority over component Sensitive Compartmented Information (SCI) policy and resources as specified in references (a), (f), and (ah).

5. <u>Policy</u>. It is DON Policy that:

a. The DON SE is an integrated framework providing central oversight, governance of, and feedback from, each security pillar: personnel, information, physical (including law enforcement policy and antiterrorism/force protection), industrial, Operations Security (OPSEC), Chemical, Biological, Radiological, Nuclear, high explosive (CBRNE), Critical Program Information (CPI) protection, Critical Infrastructure Protection (CIP), as well as coordination with SAP and SCI. The DON SE is also responsible for insider threat, identity activities, mission assurance, as well as security-related training that facilitates synchronized, seamless, and efficient implementation of programs, priorities, and initiatives of the DON SE.

b. Security is a mission critical function of the Department of Defense (DoD) and the DON. The proper execution of all security-related functions directly impacts all DON missions and capabilities, and the national defense. Therefore:

(1) The Deputy Under Secretary of the Navy(DUSN), pursuant to references (b) and (c), as the DON Security Executive, leads the DON SE and will represent the DON on the Defense Security Enterprise Executive Committee (DSE EXCOM). The DSE EXCOM, head of the DSE, governs the implementation of the Security Enterprise framework and strategic plan, in order to provide an integrated, risk-managed structure to guide security policy implementation and investment decisions, as well as provide a sound basis for oversight and evolution.

(2) The DON SE EXCOM, chaired by DUSN, will provide governance for strategic administration and policy coordination of the DON SE. The DON SE EXCOM membership and functions are described in enclosure (2) of this instruction.

(3) To the maximum extent possible, standardized security processes will be implemented and best practices identified, with appropriate provisions for unique missions and security environments across the DON SE to ensure maximum interoperability, consistent quality assurance, and cost-savings.

(4) The Chief of Naval Operations (CNO) and the Commandant of the Marine Corps (CMC) will appoint an executive leader at the General Officer/Flag Officer/Senior Executive Service (GO/FO/SES) level who will ensure service-level oversight, coordination, and implementation of security

policies, initiatives, activities, and actions. And to the extent possible, excluding SAP DON Special Access Program Central Office (SAPCO) and SCI Programs Deputy Chief of Naval Operations (DCNO N2/N6), establish one central office with sole authority and responsibility to coordinate and direct security policy formulation and provide oversight of the same, and act as a resource sponsor for security-related functions.

(5) All security programs and policies will be guided by the principle of achieving maximum efficiency, reducing redundancy, and administrative overhead, as well as identifying opportunities for cost-savings through leveraging best practices.

(6) A core of highly qualified security and management professionals, will manage execution of DON SE policy. It is desirable that DON SE Policy personnel receive appropriate certification in accordance with reference q and other sources, as applicable.

(7) DON SE investments will be guided by a capital planning and investment control process that is risk-managed, is results-based, and informs the DON's planning, programming, budgeting, and execution processes.

c. The DON SE shall measure performance in relation to DON mission impact.

(1) Security risk management practices will focus on the potential for and degree of risk of loss in relation to the cost or process burden accrued.

(2) Performance measurement requires recognition that the absence of an unwanted event may be evidence of a positive mission impact.

d. The DON will consider all means in preventing harm to its resources, to include cybersecurity, intelligence, and all security required for protection of mission assurance functions.
e. Security is the personal professional responsibility of all DON personnel (military, civilian, and contractor) and its proper implementation will be directed by commanders and other leaders at each level of the DON. It shall be fostered through awareness, education, training, and leadership.
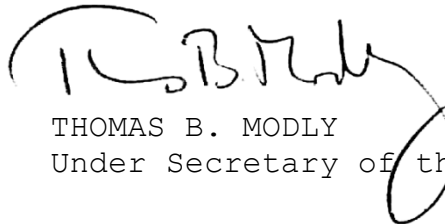
6. <u>Definitions</u>. See enclosure (4).

7. Records Management

    a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx/

    b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

8. Reports. The reporting requirements contained in enclosure (2), paragraph 6 and enclosure (4), paragraph 2 is exempt from information collection control, per reference (ak), Part IV, paragraph 7i, 7k, 7n and 7o.

THOMAS B. MODLY
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances website https://www.secnav.navy.mil/doni

REFERENCES

(a) DoD Directive 5200.43 of 1 October 2012
(b) SECNAV Memorandum, Department of the Navy Security
    Executive, 25 April 2013 (NOTAL)
(c) ALNAV 072/12, Designation of the DON Security Executive
(d) DoD Instruction 5200.01 of 21 April 2016
(e) DoD Instruction 5200.02 of 21 March 2014
(f) DoD Instruction 5200.08 of 10 December 2005
(g) DoDM 5205.02, DoD Operations Security (OPSEC) Program
    Manual of 3 April 2017
(h) DoD Instruction 5220.22 of 18 March 2011
(i) SECNAV M-5510.30B
(j) DoD Directive 5205.02E of 20 June 2012
(k) SECNAVINST 5510.36A
(l) SECNAVINST 5510.37
(m) DoD Instruction 5210.42 of 27 April 2016
(n) SECNAVINST 5510.35C
(o) SECNAVINST 8120.1C
(p) E.O. 12333
(q) DoDM 3305.13, DoD Security Accreditation and Certification
    of 14 March 2011
(r) DoD Instruction 3305.13 of 13 February 2014
(s) SECNAVINST 5430.25F
(t) DoD Directive 5134.10 of 7 May 2013
(u) DoD Directive 5124.02 of 23 June 2008
(v) DoD Directive 5118.03 of 20 April 2012
(w) DoD Directive 5144.02 of 21 November 2014
(x) SECNAVINST 5000.34F
(y) DoD Instruction 8500.01 of 14 March 2014
(z) SECNAVINST S5460.3H (NOTAL)
(aa) SECNAVINST 3030.4D
(ab) SECNAVINST 3300.2C
(ac) SECNAVINST 3501.1D
(ad) SECNAVINST 5430.107
(ae) SECNAVINST 5530.4D
(af) SECNAVINST 5500.29C
(ag) SECNAVINST 5430.7R
(ah) DoDM S-5210.41 Volumes 1-3, Nuclear Weapon Security Manual
    of 11 August 2016
(ai) Under Secretary of the Navy (UNSECNAV) Memorandum,
    Restructure of Secretariat Functions, 16 March 2018 (NOTAL)
(aj) SECNAVINST 5200.35F
(ak) SECNAV M-5214.1

DEPARTMENT OF THE NAVY SECURITY ENTERPRISE GOVERNANCE

1. <u>Purpose</u>. The DON SE governance structure will consist of two bodies: the DON SE EXCOM and DON SE Advisory Group (DON SE AG).

2. <u>Executive Committee</u>. The DON SE EXCOM will be the senior-level governance body responsible for administration, strategic guidance, and policy authority for the DON SE. In that role, the DON SE EXCOM will:

    a. Advise the DON Security Executive, pursuant to references (a) through (c), on security policy and training, provide recommendations on key policy decisions, and identify and review opportunities for standardization throughout the DON to improve effectiveness and efficiency across the DON SE. These functions include:

        (1) Development and implementation of a DON security framework that integrates all security disciplines including, but not limited to: personnel, physical, law enforcement, CPI protection, antiterrorism, force protection, industrial, information, OPSEC, CBRNE, and security training. These functions also include coordination with SAP and SCI security across all security disciplines. This framework must align with, and be informed by, other security and security-related functions, e.g., counterintelligence, nuclear physical security, foreign disclosure, security cooperation, technology transfer, export control, cybersecurity, identity activities, mission assurance, CIP, and insider threat policy.

        (2) Development of a DON mission assurance governance structure to synchronize existing protection-related risk management programs. The DON SE EXCOM will protect and ensure continued function and resilience of capabilities and assets critical to the performance of DON mission-essential functions and provide senior leaders with increased visibility and knowledge to assist in decision-making. Applicable programs include CIP, antiterrorism, continuity of operations, cybersecurity, installation emergency management, physical security, and CBRNE protection.

        (3) Development and approval of the DON security strategic plan and the monitoring and assessment of its execution.

(4) Commission of reviews and in-depth studies of security issues. Based on the results, the DON SE EXCOM will make recommendations for developing or improving policies, processes, procedures, and products to address pervasive, enduring, or emerging security challenges.

(5) Review of resources, investments and priorities, and recommendation of changes to the DON security program.

b. Provide a forum for identification, documentation, and dissemination of best practices, including those associated with security risk management, and the identification of performance measures to be used to assess the effectiveness of the DON security program and its contribution to mission success.

c. Endeavor to identify efficiencies and cost-saving measures through the identification and elimination of redundant administrative overhead, ineffective procedures, and promotion of best security practices across the DON SE.

3. <u>DON SE EXCOM Membership</u>. The voting membership of the DON SE EXCOM will consist of:

a. DUSN, who will serve as the Chair.

b. Representatives of:

(1) CNO;

(2) CMC;

(3) Assistant Secretary of the Navy (Financial Management and Comptroller) (ASN (FM&C));

(4) Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RD&A));

(5) Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN (M&RA));

(6) Assistant Secretary of the Navy (Energy, Installations and Environment) (ASN (EI&E));

(7) General Counsel of the Department of the Navy (GC);

(8) DON Chief of Information (CHINFO);

(9) DON Office of the Chief Information Officer (DON OCIO);

(10) DON/Assistant for Administration (DON/AA);

(11) DCNO (Information Warfare (N2/N6)) for SCI;

(12) Director, DON SAPCO; and

(13) Director, Naval Criminal Investigative Service (DIRNCIS).

c. Representatives, invited by the Chair from the Office of the Naval Inspector General (NAVIG) and others, as appropriate, to participate as non-voting members of the DON SE EXCOM.

d. Additional voting members, as necessary, upon recommendation to, and agreement of, the DON SE EXCOM.

4. <u>Meetings</u>. The DON SE EXCOM will meet no less than semiannually and as required at the call of the Chair. The Chair shall set the agenda with input from the members.

5. <u>DON SE AG</u>. DON SE AG, a GO/FO/SES-level body, is subordinate to the DON SE EXCOM and will formulate and coordinate all security-related policy for approval by the DON SE EXCOM

a. The DON SE AG will meet on a semiannual basis, or as needed, and will execute the strategic vision and oversee the policy set forth by the DON SE EXCOM.

b. The DON SE AG will discuss topics of interest with the DON SE EXCOM, assist in overseeing the implementation of the DON SE strategic framework, and prepare topics, as required, for the semiannual DON SE EXCOM meetings. DON SE AG membership mirrors that of the DON SE EXCOM. The Senior Director for Security and Intelligence is the Chair of the DON SE AG and may call for participation from other offices, as approve by the DON SE AG membership, or as directed by the Chair of the DON SE EXCOM.

6. <u>Subgroups and Working Groups</u>. The DON SE EXCOM and the DON SE AG may establish standing subgroups or ad-hoc working groups as deemed necessary. Each group will have a charter or specific tasking document which will include a termination date of the subgroup or working group. Meeting minutes will be maintained and agreed to by the members of the subgroup or working group and action items will be tracked. Copies of minutes and action items will be provided to the DON SE EXCOM Executive Secretary for tracking and archiving on behalf of the DON SE EXCOM. Reports of progress or actions will be provided to the DON SE EXCOM or the DON SE AG as requested.

7. <u>Administration</u>

   a. The DUSN Senior Director for Security and Intelligence shall be the Executive Secretary of the DON SE EXCOM and shall arrange meetings; prepare, coordinate, and publish minutes; track action items; and perform other duties as the Chair or DON SE EXCOM may assign, including those specified in enclosure (4).

   b. The DON SE EXCOM will establish procedures for its operation and chartering of working groups.

RESPONSIBILITIES

1. <u>UNSECNAV</u>. UNSECNAV is responsible for the oversight, management, readiness, and compliance of DON SE.

2. <u>DUSN</u>. The DUSN, serving as the DON Security Executive under the direction and control of the UNSECNAV, will:

   a. Exercise security responsibilities as described in references (a) through (c) for the development and integration of risk-managed security and protection policies and programs across the DON.

   b. Serve as the Senior Executive responsible for DON SE management, accountability, and oversight decisions, and makes security-related resource recommendations to the SECNAV.

   c. Chair the DON SE EXCOM.

   d. Advise the UNSECNAV on security policy and training matters, and provide recommendations on key policy decisions facilitating cross-functional security policy coordination.

   e. Publish and implement security instructions.

   f. Coordinate with ASN (FM&C), CNO, and CMC to identify and program security-related requirements and efficiencies.

   g. Report to and advise the UNSECNAV on the Security implications of strategic planning decisions and other significant issues raised by the DON SE EXCOM.

   h. Oversee DON security policies, plans, programs, and resources and ensure security policies and programs are aligned, designed and managed to improve performance, economy, and efficiency.

   i. Ensure DON SE has timely access to appropriate intelligence and counterintelligence products reporting threats to the DON.

   j. Ensure DON security policy and programs are implemented pursuant to applicable laws, policies, regulations, and orders, including, but not limited to, the need for a Privacy Impact Assessment and System of Records Notice prior to the retention of any records in a database.

   k. Facilitate oversight inspections by the Office of the NAVIG and other cleared officials.

   l. Provide oversight over implementation of a security framework within the DON.

   m. Serve as the Personnel Reliability Program (PRP) policy approval authority, and maintain cognizance over Director, Strategic Systems Programs implementation of PRP policy, as well as conduct all formal policy coordination external to the DON, pursuant to references (n) and (o).

   n. Provide oversight of and coordinate DON law enforcement and antiterrorism force protection policy pursuant to references (ae) through (af).

   o. Coordinate with NCIS, ASN (RD&A), ASN (FM&C), ASN (EI&E), DON SAPCO, and DON OCIO, as appropriate, to establish DON SE policy, procedures, and investment goals that align with those established for nuclear physical security, foreign disclosure, security cooperation, technology transfer, export control, cybersecurity, antiterrorism, force protection and mission assurance. Efforts shall be informed by other security- related efforts, e.g., CIP, insider threat initiatives, and CPI protection.

   p. Coordinate with ASN (M&RA) to ensure DON SE policy, procedures, and investment goals are in compliance with workforce mix, personnel policy, and procedures.

   q. Coordinate with ASN (RD&A), ASN (EI&E), ASN (FM&C), and Director, DON OCIO, as appropriate, to achieve maximum efficiency, by reducing redundancy, administrative overhead, and identifying opportunities for cost-savings by leveraging best practices.

r. In accordance with reference (aj), the establishment and use of internal controls and accounting procedures are mandated to ensure: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. Additionally, as part of the annual Manager's Internal Control Program report, the navy and Marine Corps will provide copies of the sections of their reports are that are relevant to the DON SE.

3. <u>Senior Director for Security and Intelligence (SDIR S&I)</u>. The SDIR S&I under the authority, direction of the DUSN, will serve as the DON SE AG Chair and per references (a) through (c), will:

a. Develop policy and an integrated strategic framework for the management, integration, oversight, and assessment of the DON SE.

b. Be responsible for cross-functional security integration and coordination.

c. Report to and advise the DUSN on the implications of strategic planning decisions and other security significant issues, including those identified by the DON SE EXCOM;

d. With advice from and coordination with the DON SE EXCOM, develop, maintain, and implement an integrated, cohesive DON security strategic framework; establish performance measures to assess implementation; and provide oversight to ensure compliance. In particular:

(1) Coordinate with and take guidance from the DON SE EXCOM in the development of an integrated security framework for the DON SE and recommend security policy and procedures to facilitate its implementation.

(2) Ensure the security framework includes provisions for access to integrated education, training, and professional development opportunities for security professionals.

(3) Provide guidance on, and a methodology for a DON framework that facilitates tracking security costs, estimating future years' resource requirements, measuring return on

security investments, and making risk-managed resource decisions.

(4) Develop, coordinate, maintain, and implement a DON security strategic plan that describes how the integrated security framework and the activities, functions, and processes required for its execution will be implemented, measured, and assessed.

e. On behalf of the DUSN, propose DON resource programs, formulate budget estimates, recommend resource investments and priorities, and monitor the implementation of approved programs in order to ensure adherence to approved security policy and planning guidance.

f. Provide oversight of the DON SE and the individual security disciplines, with a focus on identifying opportunities for increased standardization, improved performance, effectiveness, and efficiency.

g. Act as Executive Secretary for the DON SE EXCOM.

h. Collaborate with the Office of the Under Secretary of Defense (Intelligence), Office of the Secretary of Defense, DoD components, the Joint Staff, the Services, and the Office of the DNI, and interagency and external organizations responsible for the development and implementation of national security policy, and raise appropriate issues to the DON SE EXCOM for their consideration as necessary.

4. <u>CNO and CMC</u>. CNO and CMC will:

a. Appoint a representative at the GO/FO/SES level to serve as a DON SE EXCOM member and fulfill the responsibilities identified in enclosure (2) of this instruction.

b. Review security programs, procedures, and management structures to develop methodologies to quantify and document cost data.

c. Assist with development of the DON security framework and strategic plan.

d. Establish and maintain the Security Professional Education Development training and development program that are integrated with the DON SE policy, procedures, and investment goals.

e. Ensure DoD and DON security policies and guidance are implemented.

f. Promote proactive, informed execution of security requirements within the service, predicated upon the premise that security is everyone's responsibility, and provide oversight to confirm all service personnel understand their roles and responsibilities in ensuring DON security.

g. Establish programs to hire, train, and retain a professional security workforce consistent with this instruction and references (q) and (r).

h. Align service security investment portfolio with DSE and DON SE policies and guidance.

i. The GO/FO/SES level designated single service security program executive will.

   (1) Have knowledge of the security disciplines within the DSE and DON SE necessary to facilitate and oversee implementation of the DSE and DON SE security framework and strategic plans and the requirements of this directive within the service.

   (2) Provide leadership for and maintain cognizance over the service's process for resourcing its security program, to ensure adequate investment of resources to support an integrated security program, and provide information on those efforts as requested by the DON SE EXCOM Chair.

   (3) Share cost, schedule, and performance data regarding the service's security program and investments with the DON SE EXCOM as needed for execution of its responsibilities.

j. Designate appropriate personnel for sub-groups when requested by the DON SE EXCOM Chair.

k. Identify efficiencies, redundancies, unnecessary administrative overhead, and opportunities for remediation to achieve cost-savings through leveraging best practices and other measures.

5. ASN (RD&A). The ASN (RD&A) will:

a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b. Assist with development of the DON security framework and strategic plan.

c. Provide advice to the DON SE and the DON SE EXCOM within assigned areas of responsibility, including procurement policy and Defense Industrial Base implementation.

d. Identify efficiencies, redundancies, unnecessary administrative overhead, and opportunities and identify remediation to achieve cost-savings through leveraging best practices and other measures.

e. Ensure policies, decisions, and recommendations regarding modifications in security policy, programs, and initiatives are issued and implemented across the Research Development Test and Evaluation Federal and contract constituencies.

f. Assist with development of CPI protection governance structure, to include applicable strategy, policy, and procedure for CPI identification and program protection planning.

6. ASN (M&RA). The ASN (M&RA) will:

a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b. Assist with development of the DON security framework and strategic plan.

c. Provide advice, as necessary or requested, to the DON SE and DON SE EXCOM on civilian and military personnel issues, including those related to position sensitivity designation, performance standards, and evaluation criteria.

d.   Program and plan for security-related education, training, support, and oversight requirements.

e.   Ensure requirements, training, and standards are issued to Reserve and Active Components.

f.   Support development and execute a methodology for identifying and documenting DON security positions.

7.   <u>ASN (FM&C)</u>. The ASN (FM&C) will:

a.   Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b.   Assist with development of the DON security framework and strategic plan.

c.   Provide advice, to the DON SE and DON SE EXCOM on issues related to security funding, costs, and performance measures.

d.   Review DON resources, billet structure, and overhead to identify potential efficiencies, reduce redundancy, and achieve cost-savings.

e.   Endeavor to identify efficiencies, redundancies, unnecessary administrative overhead, opportunities, and remediation to achieve cost-savings through leveraging best practices and other measures.

8.   <u>ASN (EI&E)</u>. The ASN (EI&E) will:

a.   Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b.   Assist with development of the DON security framework and strategic plan.

c.   Support development of a methodology for identifying, documenting, and quantifying security positions and costs.

9. <u>DON/AA</u>. The DON/AA will:

a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b. Provide advice, to the DON SE and DON SE EXCOM.

c. Provide leadership for and maintain cognizance over the SECNAV Special Security Office and collateral security functions.

10. <u>GC</u>. The GC will:

a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b. Provide legal advice and counsel, to the DON Security Executive and DON SE EXCOM.

11. <u>Director, DON OCIO</u>. The Director, DON OCIO will:

a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b. Assist with development of the DON security framework and mission assurance governance structure, to include applicable strategy, policy, procedures, and investment goals, as the DON office of primary responsibility for cybersecurity.

12. <u>DIRNCIS</u>. The DIRNCIS, as the Senior Official for Criminal Investigations and Counterintelligence, will:

a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

b. Assist with development of the DON security framework and strategic plan.

c. Provide advice, as necessary or requested, to the DON SE and DON SE EXCOM on investigative, law enforcement, antiterrorism, technical surveillance countermeasures, and counterintelligence programs within the DON.

13. <u>DON SAPCO</u>. The Director, DON SAPCO will:

    a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

    b. Assist with development of the DON security framework and strategic plan.

    c. Develop SAP security policy that is coordinated with the DON SE EXCOM as appropriate.

14. <u>DCNO N2/N6 for SCI</u>. The DCNO N2/N6 will:

    a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

    b. Assist with development of the defense security framework and strategic plan and coordinate with the DUSN to establish SCI policy that aligns with the DON SE policy, procedures, and investment goals.

15. <u>CHINFO</u>. The CHINFO will:

    a. Appoint a representative at the GO/FO/SES level to serve on the DON SE EXCOM.

    b. Assist with development of the DON security framework and strategic plan.

    c. Provide public affairs and communication advice and counsel to the DON SE and DON SE EXCOM.

16. In addition to responsibilities listed above, <u>all members of the DON SE</u> are responsible for supporting enhanced accountability and documentation of security costs, capturing and communicating capability shortfalls, and maintaining an active OPSEC posture.

DEFINITIONS

1. <u>Antiterrorism</u>. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. Antiterrorism measures are taken to detect, deter, defend, defeat, and mitigate acts of terror.

2. <u>CIP</u>. Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc. (Source: JP 1-02).

3. <u>CPI</u>. U.S. capability elements that contribute to warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment.

4. <u>DON SE</u>. An integrated framework providing central oversight, governance of, and feedback from, each security pillar: personnel, information, physical (including law enforcement policy and antiterrorism/force protection), industrial, OPSEC, CBRNE, CPI protection, insider threat, identity activities, CIP, as well as coordination with SAP and SCI. The DON SE is also responsible for mission assurance, as well as security-related training that facilitates synchronized, seamless, and efficient implementation of security relevant DON programs, priorities, and initiatives.

5. <u>DON SE Program</u>. The programmatic planning, expenditures, and return on investment estimating process for the DON SE.

6. <u>Identity Activities</u>. A collection of functions and actions that appropriately recognize and differentiate one entity from another to support decision making. Activities include the collection of identity attributes and captured

materials, their processing and exploitation, all-source analytic efforts, and production and dissemination of identity intelligence products to inform policy and strategy development, operational planning and assessment, and appropriate action at the point of encounter.

7. Industrial Security. A multi-disciplinary security program concerned with the protection of classified information developed by or entrusted to U.S. industry.

8. Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

9. Information Security. The security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information that is authorized protection by executive order, statute, or regulation. Information security includes protection of classified, controlled unclassified, and SCI.

10. Insider Threat. A threat presented by a person who:

    a. Has, or once had, authorized access to information, a facility, network, person, or resource of the Department.

    b. Wittingly, or unwittingly, commits:

        (1) An act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities.

        (2) A destructive act, which may include physical harm to another in the workplace.

11. OPSEC. A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to:

    a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk.

c. Select and execute countermeasures that eliminate or reduce to an acceptable level the risks to friendly actions and operations or reduce it to an acceptable level.

12. Personnel Security. The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.

13. Physical Security. Security concerned with physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and defend them against espionage, sabotage, damage, and theft.

14. Research, Development, and Acquisition Protection. The safeguarding of selected research, technology, information, and associated support systems, during the research, development, test, evaluation, and acquisition processes.

15. Security. Proactive measures employed to safeguard personnel, information, operations, resources, technologies, facilities, and other items deemed vital against harm, loss, or hostile acts and influences.

16. Security Framework. Structure or architecture describing how security disciplines relate to and interact with each other.

17. Security Professional. A functional career occupation in which the incumbent executes or manages Federal Government agency or Industrial Security programs and related security activities, ensuring compliance with government security policies, directives, and procedures. Examples of responsibilities and position titles include: Activity Security Manager, Chief Security Officer, Field Security Officer, Area Security Officer, Special Security Representative, Program Security Officer, or Security Guard.

18. <u>SCI</u>. Classified national intelligence concerning or derived from intelligence sources and/or methods that must be protected within formal control systems established and overseen by the DNI.

19. <u>SAP</u>. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.